

Россиянам рассказали, как борются с хакерами и почему противостояние никогда не закончится

Количество сложных кибератак на крупные компании с начала 2024 года выросло на 60%, сообщает RED Security. Больше всего от действий [хакеров](#) пострадали промышленность, финансы и телеком. Эксперты прогнозируют, что в 2025 году атаки станут ещё сложнее и изощрённее. Александр Щетинин, CEO компании Xello, отметил, что [хакеры](#) часто опережают IT-безопасность, используя уязвимости, искусственный интеллект и методы социальной инженерии.

Для защиты от злоумышленников сегодня активно применяются технологии киберобмана. Например, компании создают фальшивые учётные записи, базы данных и сети, которые привлекают [хакеров](#). Эти ловушки помогают задержать злоумышленника и обнаружить его действия. Особое внимание уделяется поведению [хакеров](#) внутри сети: они стараются не вызывать подозрений, перемещаясь по узлам и медленно собирая данные.

Одной из самых эффективных технологий называют психологический киберобман. Он основан на том, чтобы заставить [хакеров](#) подозревать наличие ловушек. Исследования показывают, что такая тактика делает злоумышленников более осторожными и увеличивает вероятность их ошибок. В сочетании с техническими методами киберобман помогает не только защищать данные, но и предотвращать серьёзные сбои в системах.